Rzeczpospolita Polska
Ministerstwo Klimatu i Środowiska
Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”

Podręcznik kontroli organu właściwego ds. cyberbezpieczeństwa sektora energii względem operatorów usług kluczowych

styczeń 2023

Organ właściwy ds. cyberbezpieczeństwa sektora energii

Ministerstwo Klimatu i Środowiska

Spis treści

1. Podstawy prawne

Akty prawne i dokumenty krajowe:

Ustawa z dnia 5 lipca *o krajowym systemie cyberbezpieczeństwa* (tj. Dz.U. z 2022 r. poz. 1863).

Ustawa z dnia 6 marca 2018 r. - *Prawo przedsiębiorców* (tj. Dz.U. z 2021 r., poz. 162).

Ustawa z dnia 15 lipca 2011 r. *o kontroli w administracji rządowej* (tj. Dz.U. z 2020 r., poz. 224).

Ustawa z dnia 10 kwietnia 1997 r. *Prawo energetyczne* (tj. Dz.U. z 2022 r. poz. 1385).

Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (tj. Dz.U. z 2022 r. poz. 261).

Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. *w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych* (Dz. U. z 2018 r. poz. 1806).

Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. *w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej* (Dz.U. z 2018 r. poz. 2080)

Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. *w sprawie progów uznania incydentu za poważny* (Dz.U. z 2018 r. poz. 2180)

Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo* (Dz.U. z 2019 r. poz. 2479)

Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. *w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu* (Dz.U. z 2018 r. poz. 1999)

Rekomendacje Ministra Klimatu i Środowiska dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów, wrzesień 2021 r.

Akty prawne międzynarodowe:

Zalecenie Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. *w sprawie cyberbezpieczeństwa w sektorze energetycznym* (notyfikowana jako dokument nr C(2019) 2400),

2. Cel i zakres podręcznika

Zgodnie z art. 53 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o *krajowym systemie cyberbezpieczeństwa* (dalej jako UKSC) nadzór w zakresie stosowania przepisów ustawy sprawują organy właściwe do spraw cyberbezpieczeństwa, w zakresie wykonywania przez operatorów usług kluczowych obowiązków wynikających z UKSC, dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych. W przypadku sektora energii, zgodnie z art. 41 pkt. 1 UKSC organem właściwym ds. cyberbezpieczeństwa jest Minister Klimatu i Środowiska. Celem podręcznika jest

doprecyzowanie kwestii proceduralnych dotyczących przeprowadzania kontroli operatorów usług kluczowych nadzorowanych przez Ministra Klimatu i Środowiska. Podręcznik określa katalog minimalnych obowiązków weryfikowanych przez organ nadzorczy, których spełnienie oznacza wdrożenie przez podmiot zobowiązany środków na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa, a także zgłaszania incydentów poważnych.

Podmioty kontrolowane dzielą się na dwie grupy: przedsiębiorców i podmioty niebędące przedsiębiorcami. W zależności, do której grupy dany operator zostanie włączony, kontrola jest przeprowadzana na podstawie następujących przepisów prawnych:

1) do podmiotów będących przedsiębiorstwami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (dalej jako UPP),
2) względem operatorów niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, określające zasady i tryb przeprowadzania kontroli.

W przypadku sektora energii, gdzie na chwilę obecną wszyscy wyznaczeni operatorzy usług kluczowych to przedsiębiorstwa, kontrole prowadzi się na podstawie ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (tj. Dz.U. z 2021 r., poz. 162). Z tego powodu niniejszy podręcznik odnosi się do kontroli przeprowadzanej na gruncie UPP.

3. Definicje i stosowane oznaczenia

Administrator Systemu – osoba zarządzająca systemem teleinformatycznym, dbająca o jego sprawne oraz bezpieczne działanie i wykorzystywanie, a także odpowiedzialna za zapewnienie jego ciągłości działania.

Aktywa – urządzenia, systemy, obiekty, informacje i dane, procesy, dokumentacja, które umożliwiają organizacji osiągnięcie celów biznesowych. Jako aktywa rozumie się także kompetencje pracowników organizacji uwzględnionych w systemie zarządzania bezpieczeństwem.

Aktywa informacyjne – dane i informacje, które umożliwiają organizacji osiągnięcie celów biznesowych.

BCP – (ang. *Business Continuity Plans; pl. Plany Ciągłości Działania*) – tworzenie, modyfikacja, aktualizacja planów wznawiania działania procesów.

Bezpieczeństwo informacji – zachowanie atrybutów bezpieczeństwa, w tym poufności, integralności, autentyczności i dostępności informacji.

Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

ICS/IACS – (ang. *Industrial Control Systems* lub *Industrial Automation and Control System*) – systemy teleinformatyczne, które realizują funkcje nadzoru, zarządzania, sterowania, regulacji, pomiaru, monitoringu, bezpieczeństwa (lub kilku tych funkcji łącznie) dla procesów technologicznych i przemysłowych. Systemy ICS są częścią szeroko pojętego OT.

Incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;

IT – (ang. *Information Technology*) – wszelkie działania związane z wykorzystaniem urządzeń informatycznych oraz usług im towarzyszących, a także gromadzenie, przetwarzanie, udostępnianie informacji w formie elektronicznej z wykorzystaniem technik cyfrowych i wszelkich narzędzi komunikacji elektronicznej.

MKiŚ – Ministerstwo Klimatu i Środowiska, organ właściwy ds. cyberbezpieczeństwa sektora energii

Operator infrastruktury krytycznej – właściciel, posiadacz samoistny albo posiadacz zależny obiektów, instalacji urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*.

Operator usługi kluczowej (OUK) – jest to podmiot, o którym mowa w załączniku nr 1 do UKSC, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do UKSC.

OT – (ang. *Operational Technology*) – sprzęt i oprogramowanie wykorzystywane do sterowania i nadzoru nad procesami technologicznymi i produkcyjnymi.

Podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa.

Ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.

SCADA – (ang. *Supervisory Control and Data Acquisition*) – system informacyjny nadzorujący przebieg procesu technologicznego lub produkcyjnego obejmujący zbieranie aktualnych danych (pomiarów), ich wizualizację, sterowanie procesem, alarmowanie oraz archiwizację danych.

System informacyjny – system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i 1544), wraz z przetwarzanymi w nim danymi w postaci elektronicznej.

System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

UKSC - ustawa z dnia 5 lipca *o krajowym systemie cyberbezpieczeństwa* (tj. Dz.U. z 2022 r. poz. 1863).

UPP – ustawa z dnia 6 marca 2018 r. *Prawo przedsiębiorców* (tj. Dz.U. z 2021 r., poz. 162).

Usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych.

Użytkownik – upoważniona osoba fizyczna (pracownik, współpracownik, kontrahent lub osoba działająca w imieniu i na rzecz kontrahenta) korzystająca z systemów teleinformatycznych Spółki.

Zagrożenie cyberbezpieczeństwa – potencjalna przyczyna wystąpienia incydentu.

4. Podmioty uprawnione do kontroli

Zgodnie z art. 42 ust. 1 pkt 8 UKSC, organ właściwy do spraw cyberbezpieczeństwa prowadzi kontrole operatorów usług kluczowych.

Szczegółowe wymagania dotyczące uprawnień osób kontrolujących, a także obowiązki podmiotu kontrolowanego zostały wskazane w UKSC.

UPRAWNIENIA OSOBY KONTROLUJĄCEJ

Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do:

1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki;
2) wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej;
3) sporządzania, a w razie potrzeby żądania sporządzenia, niezbędnych do kontroli kopii, odpisów lub wyciągów z dokumentów oraz zestawień lub obliczeń;
4) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli;
5) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu kontroli;
6) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych.

Osoba kontrolująca składa oświadczenie o zachowaniu bezstronności i poufności – wzór dokumentu stanowi załącznik nr 5.

OBOWIĄZKI PODMIOTU KONTROLOWANEGO

Kontrolowane podmioty będące przedsiębiorcami zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli, w szczególności przez:

- zapewnienie niezwłocznego przedstawienia żądanych dokumentów,
- terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą,
- udostępniania niezbędnych urządzeń technicznych, a także
- sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych.

Obowiązkiem kontrolowanego jest terminowe udzielanie wyjaśnień w sprawach objętych kontrolą. Żądanie złożenia wyjaśnień może zostać skierowane do każdego pracownika podmiotu kontrolowanego, w tym również do kierownika jednostki kontrolowanej. Wyjaśnienia z reguły dotyczą okoliczności towarzyszących odkrytym nieprawidłowościom i mogą mieć formę pisemną, gdy przedstawiciel podmiotu kontrolowanego sam sporządza wyjaśnienia i przekazuje je kontrolerom, bądź ustną, kontroler spisuje w formie protokołu wyjaśnienia przekazane przez przedstawiciela podmiotu kontrolowanego, podpisywanego następnie przez obydwie strony.

Podmiot kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków. W przypadku odmowy potwierdzenia za zgodność z oryginałem potwierdza je osoba prowadząca czynności kontrolne, o czym czyni wzmiankę w protokole kontroli.

Dobrą praktyką podczas czynności kontrolnych będzie wyznaczenie przez podmiot kontrolowany pracownika będącego punktem kontaktowym dla kontrolerów, który również odpowiada za realizację obowiązków kontrolowanego wynikających z UKSC.

5. Przedmiot kontroli

Zgodnie z UPP, przedmiot kontroli ustala się na podstawie przeprowadzonej analizy prawdopodobieństwa naruszenia prawa w ramach wykonywania działalności gospodarczej (patrz rozdział 8 – Ryzyko naruszeń).

Kontrola powinna opierać się o podejście bazujące na ryzyku (ang. *risk-based*), które służy do zbadania obszarów generujących największe ryzyko dla organizacji. Wymaga to zrozumienia organizacji i jej środowiska, w tym:

- zewnętrznych i wewnętrznych czynników mających wpływ na organizację,
- wyboru i stosowania przez organizację polityk i procedur,
- celów i strategii organizacji,
- pomiaru i przeglądu wyników organizacji.

Ponadto, należy również przeanalizować i zrozumieć:

- strategię zarządzania podmiotem,
- produkty i usługi biznesowe,
- proces zarządzania firmą,
- typy transakcji, partnerów biznesowych i przepływy transakcji w systemach informacyjnych.

Zatem, w podejściu opartym na ryzyku należy najpierw zebrać informacje o podmiocie (jaką działalność prowadzi, jakie jest jego otoczenie biznesowe i prawne, sprawdzić czy były przeprowadzone audyty, sprawdzić czy istnieje jakieś ryzyko wbudowane w daną branżę np. ryzyko kursowe dla handlu z zagranicą itd.), a następnie dokonać analizy prawdopodobieństwa naruszenia prawa w ramach wykonywanej działalności gospodarczej (art. 47 UPP).

Na podstawie powyższych działań, a zwłaszcza zidentyfikowania obszarów, w których operator usług kluczowych nie spełnia wymogów wskazanych w UKSC i aktach wykonawczych, należy zdefiniować zakres kontroli, czyli jasno wskazać co będzie sprawdzał podmiot kontrolujący. Należy pamiętać, że zakres kontroli zawsze musi się wpisywać w regulacje wskazane w UKSC i akty wykonawcze pod kątem obowiązków OUK oraz w ustawie – Prawo Przedsiębiorców, w odniesieniu do przepisów regulujących zasady prowadzenia kontroli u przedsiębiorców.

Przedmiotem kontroli jest wdrożenie przez podmiot zobowiązany środków na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa, a także zgłaszania incydentów poważnych. Kontrola Ministerstwa Klimatu i Środowiska dotyczy podjętych działań służących zapewnieniu odporności systemów informacyjnych operatorów usług kluczowych w energetyce, na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

W świetle UKSC, system informacyjny należy definiować na podstawie art. 2 pkt 14 UKSC, zgodnie z którym system informacyjny to *system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne)*[1]*, wraz z przetwarzanymi w nim danymi w postaci elektronicznej*. Zgodnie z art. 3 pkt 3 ustawy o informatyzacji, system teleinformatyczny to *zespół współpracujących ze sobą urządzeń*

[1] Dz.U. z 2020 r. poz. 346, 568 i 695, dalej: ustawa o informatyzacji.

informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy Prawo telekomunikacyjne (ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne)[2]. Telekomunikacyjne urządzenie końcowe to natomiast *urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci* (art. 2 pkt 43 Prawa telekomunikacyjnego).

Zgodnie z powyższym, system informacyjny ma zapewniać przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci komputerowe za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego. Definicja opisuje więc trzy funkcjonalności systemu – przetwarzanie, przechowywanie oraz wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą urządzenia końcowego. Przepis nie wskazuje, aby wszystkie trzy funkcjonalności musiały być zapewnione przez system jednocześnie.

W celu odpowiedniego zidentyfikowania systemów informacyjnych stosowanych w sektorze energii, będących przedmiotem kontroli, należy wyróżnić pięć kategorii funkcjonalnych:

1) operacyjną,
2) biznesową,
3) bezpieczeństwa (*safety*),
4) ochrony fizycznej (*security*),
5) reagowania kryzysowego.

Każda z nich obejmuje różne zadania systemów. Zatem, kiedy jest mowa o kategorii operacyjnej należy przez to rozumieć systemy kontroli procesu, w tym systemy oprzyrządowania i kontroli (I&C – ang. *Instrumentation and Control Systems*), sterownie systemów I&C zawierające systemy alarmowe, systemy komputerowe wykorzystywane do zbierania i przygotowania odpowiednich informacji na potrzeby sterowni, systemy do obsługi i przechowywania paliw, systemy zarządzania konfiguracją oraz utrzymania, zdalny dostęp i VPN (ang. *Virtual Private Network*) do środowiska operatorskiego, infrastruktura służąca do komunikacji głosowej i transmisji danych, infrastruktura operatorska i systemy kontroli, środowiska testowe i programistyczne dla systemów operacyjnych.

Jeżeli chodzi o systemy biznesowe, to dotyczą ona takich aspektów jak: infrastruktura komunikacji głosowej i transferu danych, systemy służące do zarządzania zasobami ludzkimi i repozytoria danych, systemy techniczne i inżynierskie, systemy zlecania pracy i pozwolenia na pracę, systemy zamówień publicznych oraz systemy biurowe.

Do systemów kategorii bezpieczeństwa (*safety*) zalicza się systemy ochrony, systemy wykonujące działania zabezpieczające, uruchamiane przez systemy bezpieczeństwa bądź ręcznie, systemy wspomagające system bezpieczeństwa, w tym systemy zasilania awaryjnego.

W zakres kategorii ochrony fizycznej wchodzą takie systemy, jak: systemy monitoringu wizyjnego i wykrycia włamania, systemy kontroli dostępu, systemy kontroli zasobów, infrastruktura służąca do przesyłania głosu i danych, systemy alarmowe, a także bazy danych zawierające informacje o posiadanych przez pracowników poświadczeniach bezpieczeństwa, używane w celu zapewnienia, że personel ma przyznany dostęp do danej strefy.

[2] Dz.U. z 2021 r. poz. 576, dalej: Prawo telekomunikacyjne.

Ostatnią kategorię stanowią systemy służące do reagowania kryzysowego takie, jak: systemy monitorowania środowiska, systemy monitorujące promieniowanie jądrowe lub elektromagnetyczne, systemy ochrony przeciwpożarowej oraz środki komunikacji umożliwiające transmisję głosu i danych.

Wymienione wyżej rodzaje systemów wchodzących w poszczególne kategorie funkcjonalne nie stanowią zbioru zamkniętego i w niektórych organizacjach przytoczona systematyka może być bardziej zróżnicowana. Jednakże pewne podstawy są wspólne dla wszystkich podmiotów z sektora energii.

W toku kontroli w szczególności analizowane są systemy informacyjne wskazane przez podmiot w toku procedury art. 43 ust. 1 UKSC.

6. Planowanie kontroli

Kontrole planuje się i przeprowadza po uprzednim dokonaniu analizy prawdopodobieństwa naruszenia prawa w ramach wykonywania działalności gospodarczej (art. 47 UPP). Analiza ta obejmuje identyfikację obszarów podmiotowych i przedmiotowych, w których ryzyko naruszenia przepisów jest największe. Sposób przeprowadzenia analizy określa organ kontroli lub organ nadrzędny.

Procedura nie ma zastosowania:

1) w przypadku, gdy Ministerstwo Klimatu i Środowiska poweźmie uzasadnione podejrzenie:
    a. zagrożenia życia lub zdrowia,
    b. popełnienia przestępstwa lub wykroczenia,
    c. popełnienia przestępstwa skarbowego lub wykroczenia skarbowego,
    d. innego naruszenia prawnego zakazu lub niedopełnienia prawnego obowiązku – w wyniku wykonywania działalności gospodarczej objętej kontrolą;

2) w przypadku, gdy jest ona niezbędna do przeprowadzenia postępowania w celu sprawdzenia wykonania zaleceń pokontrolnych organu, wykonania decyzji albo postanowień nakazujących usunięcie naruszeń prawa, w związku z przeprowadzoną kontrolą, albo do sprawdzenia wykonania wezwania, o którym mowa w art. 21a ust. 1, zobowiązania, o którym mowa w art. 21a ust. 2, lub weryfikacji powiadomienia, o którym mowa w art. 21a ust. 5 lub 6 UPP.

W Biuletynie Informacji Publicznej na stronie Ministerstwa Klimatu i Środowiska[3] zamieszczono ogólny schemat procedur kontroli wynikający z przepisów ustawy *o krajowym systemie cyberbezpieczeństwa*.

Dla każdej kontroli sporządza się harmonogram kontroli, stanowiący załącznik nr 6 do podręcznika.

Ponadto, Ministerstwo Klimatu i Środowiska prowadzi Rejestr Kontroli OUK na dany rok kalendarzowy, który zawiera informację o przeprowadzonych kontrolach, czasie ich trwania, zakresie, ewentualnych uwagach oraz wytworzonych dokumentach. Wzór rejestru kontroli stanowi załącznik nr 9.

7. Cele i rodzaje zabezpieczeń

Ustawa o krajowym systemie cyberbezpieczeństwa wraz z aktami wykonawczymi definiuje wymogi, które operatorzy usług kluczowych mają obowiązek wdrożyć w swojej organizacji.

[3] https://bip.mos.gov.pl/kontrole/kontrole-operatorow-uslug-kluczowych/ogolny-schemat-kontroli/

W załączniku nr 1 do niniejszego podręcznika – „*Przykładowe dokumenty wskazane w regulacjach*”, zostały wymienione wymagania wskazane w UKSC wraz z przykładami dokumentacji potwierdzającymi, że dany warunek został spełniony przez operatora usługi kluczowej. Katalog dokumentacji nie jest zamknięty, ponieważ każdy podmiot może w różny sposób adresować dany obowiązek i tym samym inaczej regulować daną kwestię wewnętrznie.

Jako przykład, artykuł 8 UKSC wskazuje, że operator ma mieć wdrożony system zarządzania bezpieczeństwem w systemie informacyjnym. W związku z tym, podczas kontroli OUK kontroler powinien dokonać weryfikacji dokumentacji, która potwierdzi, że ten warunek jest realizowany. Może to być np. przyjęta przez kierownictwo Polityka Bezpieczeństwa Informacji, a więc dokument ustanawiający system zarządzania bezpieczeństwem w systemie informacyjnym, procedura nadzoru nad systemem zarządzania bezpieczeństwem w systemie informacyjnym itd.

Należy również mieć na uwadze, że w UKSC są obowiązki, których niespełnienie nie spowoduje nałożenia na operatora usługi kluczowej kary pieniężnej. Mowa tu na przykład o obowiązku wskazanym w art. 8 pkt 3, który mówi o tym, że wdrożony u OUK system zarządzania bezpieczeństwem w systemie informacyjnym ma uwzględniać zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Jeżeli operator nie ma wdrożonej takiej funkcjonalności systemu zarządzania bezpieczeństwem w systemie informacyjnym, wówczas Ministerstwo Klimatu i Środowiska jako organ właściwy ds. cyberbezpieczeństwa nie ma podstawy prawnej do nałożenia kary pieniężnej.

Ustawodawca nałożył również konkretne obowiązki na struktury wewnętrzne i zewnętrzne odpowiedzialne za cyberbezpieczeństwo. Kwestie te reguluje rozporządzenie Ministra Cyfryzacji z 4 grudnia 2019 r*. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*. Zgodnie z tym dokumentem, warunki które muszą zostać spełnione przez struktury odpowiedzialne za cyberbezpieczeństwo należy podzielić na:

- organizacyjne,
- techniczne,
- zabezpieczenia pomieszczeń,
- zabezpieczenia informacji,
- zdalnego wykonywania usług z zakresu cyberbezpieczeństwa.

Ponadto, zgodnie z rozporządzeniem Rady Ministrów z dnia 16 października 2018 r. *w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,* operator usługi kluczowej ma również obowiązek posiadać:

- dokumentację dotyczącą systemu zarządzania bezpieczeństwem informacji, która jest wytworzona zgodnie z wymaganiami normy PN-EN ISO/IEC 27001,
- dokumentację ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa,
- dokumentację systemu zarządzania ciągłością działania usługi kluczowej, wytworzoną zgodnie z wymaganiami normy PN-EN ISO 22301,
- dokumentację techniczną systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,
- dokumentację wynikającą ze specyfiki świadczonej usługi kluczowej w danym sektorze lub podsektorze, a także
- dokumentację operacyjną.

W załączniku nr 1 do podręcznika zostały wskazane przykładowe rodzaje wymaganej dokumentacji.

8. Ryzyko naruszeń

W celu przeprowadzenia analizy prawdopodobieństwa naruszenia prawa w ramach wykonywania działalności gospodarczej przez przedsiębiorcę, Ministerstwo Klimatu i Środowiska przed wszczęciem kontroli analizuje szereg informacji, które dają wiedzę na temat sposobu realizowania przez OUK obowiązków określonych w UKSC. Na te potrzeby, organ właściwy ds. cyberbezpieczeństwa dla sektora energii prowadzi elektroniczną ewidencję realizacji wymagań cyberbezpieczeństwa (w formie tabeli), służącą ocenie zarządzania cyberbezpieczeństwem przez operatorów usług kluczowych w sektorze energii. Tabela jest uzupełniana w oparciu o niżej wymienione informacje ze sprawozdań z audytu bezpieczeństwa systemu informacyjnego, dokumentacji z szacowania ryzyka oraz formularza dojrzałości organizacji pod kątem cyberbezpieczeństwa. W oparciu o te dane sporządzana jest zbiorcza ocena operatora usługi kluczowej pod kątem realizacji wymagań z zakresu cyberbezpieczeństwa, jak i tworzony jest również „ranking" realizacji wymagań z zakresu cyberbezpieczeństwa.

SPRAWOZDANIE Z AUDYTU BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO

Zgodnie z art. 15 ust. 1 UKSC, operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Operator usługi kluczowej przekazuje kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek organu właściwego do spraw cyberbezpieczeństwa (art. 15 ust. 7 pkt. 1). Po przekazaniu sprawozdania przez OUK, jest ono poddawane analizie pod kątem zgodności przeprowadzonych czynności z wymaganiami formalnymi, dotyczącymi audytu zawartymi w UKSC.

Wymagania formalne dotyczące audytu:

- jest on przeprowadzany w terminie:
  - roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej,
  - następnie co najmniej raz na 2 lata,
- dotyczy bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,
- jest przeprowadzony przez odpowiedni podmiot – jednostkę oceniającą zgodność lub co najmniej dwóch audytorów lub sektorowy zespół cyberbezpieczeństwa zgodnie z art. 15 ust. 2 i 3.

Wyjątek stanowi art. 15 ust. 6 UKSC, gdyż w przypadku przeprowadzenia w danym roku przez operatora usługi kluczowej audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o *informatyzacji działalności podmiotów realizujących zadania publiczne*, w stosunku do systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez osoby spełniające warunki określone w ust. 2 pkt 2, nie ma on obowiązku przeprowadzania audytu przez 2 lata.

Ponadto, w kontekście sprawozdania z audytu, poza wymogami formalnymi, organ właściwy bierze pod uwagę także zawarte w nim informacje merytoryczne, m.in. dotyczące funkcjonowania obszarów objętych audytem, jego kryteriów oraz ewentualnych zaleceń poaudytowych. Stanowią one dodatkowe źródło informacji w zakresie funkcjonowania wdrożonego systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, wykonywania działalności gospodarczej przez przedsiębiorcę oraz realizowania pozostałych obowiązków operatora usługi kluczowej.

DOKUMENTACJA DOTYCZĄCA SZACOWANIA RYZYKA

Jednym z obowiązków operatora usługi kluczowej, wymienionym w art. 8 pkt. 1 UKSC, jest prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem. Obowiązek ten jest związany także z art. 10 ust. 1, według którego OUK opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, a także rozporządzeniem[4] wskazującym rodzaje tej dokumentacji.

Analiza ww. dokumentacji stanowi również źródło informacji dotyczących realizowania obowiązków OUK przez przedsiębiorcę, jak i wykonywania przez niego działalności gospodarczej. Ponadto, ustawa nakazuje realizację dodatkowych obowiązków związanych z postępowaniem z dokumentacją, w celu zapewnienia:

- dostępności dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami,
- ochrony dokumentów przed niewłaściwym użyciem lub utratą integralności,
- oznaczania kolejnych wersji dokumentów umożliwiającego określenie zmian dokonanych w tych dokumentach.

Należy podkreślić, iż systematyczne szacowanie ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem przez OUK stanowi jeden z najważniejszych jego obowiązków, gdyż pozwala uzyskać świadomość sytuacyjną w zakresie incydentów możliwych do wystąpienia oraz pozwala opracować i wdrożyć odpowiednie środki polegające na przeciwdziałaniu im. Podstawą wystąpienia Ministerstwa Klimatu i Środowiska o tego typu dokumentację jest art. 42 ust 1 pkt. 6 UKSC.

FORMULARZ DOJRZAŁOŚCI ORGANIZACJI POD KĄTEM CYBERBEZPIECZEŃSTWA

Załącznikiem nr 1 do rekomendacji sektorowych Ministra Klimatu i Środowiska w zakresie cyberbezpieczeństwa[5] jest wzór formularza weryfikacji dojrzałości cyberbezpieczeństwa organizacji. Został on oparty o ramy doskonalenia cyberbezpieczeństwa dla infrastruktury krytycznej opracowane przez amerykański Narodowy Instytut Standardów i Technologii (ang. *National Institute of Standards and Technology*, NIST). Jego celem jest wsparcie procesu szacowania ryzyka wystąpienia incydentu cyberbezpieczeństwa w systemach informacyjnych służących do świadczenia usługi kluczowej oraz pomoc w określeniu poziomu dojrzałości organizacji w zakresie cyberbezpieczeństwa, który może okazać się pomocny również przy prowadzeniu samego procesu szacowania tego ryzyka oraz opracowywaniu katalogu stosowanych zabezpieczeń.

Po uzupełnieniu formularza przez OUK, staje się on źródłem informacji w zakresie wielu obszarów zarówno organizacyjnych, jak i technicznych, w kontekście funkcjonowania organizacji, których analiza pozwala oszacować prawdopodobieństwo naruszenia prawa w ramach wykonywania działalności

[4] Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. *w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej* (Dz.U. z 2018 r. poz. 2080).

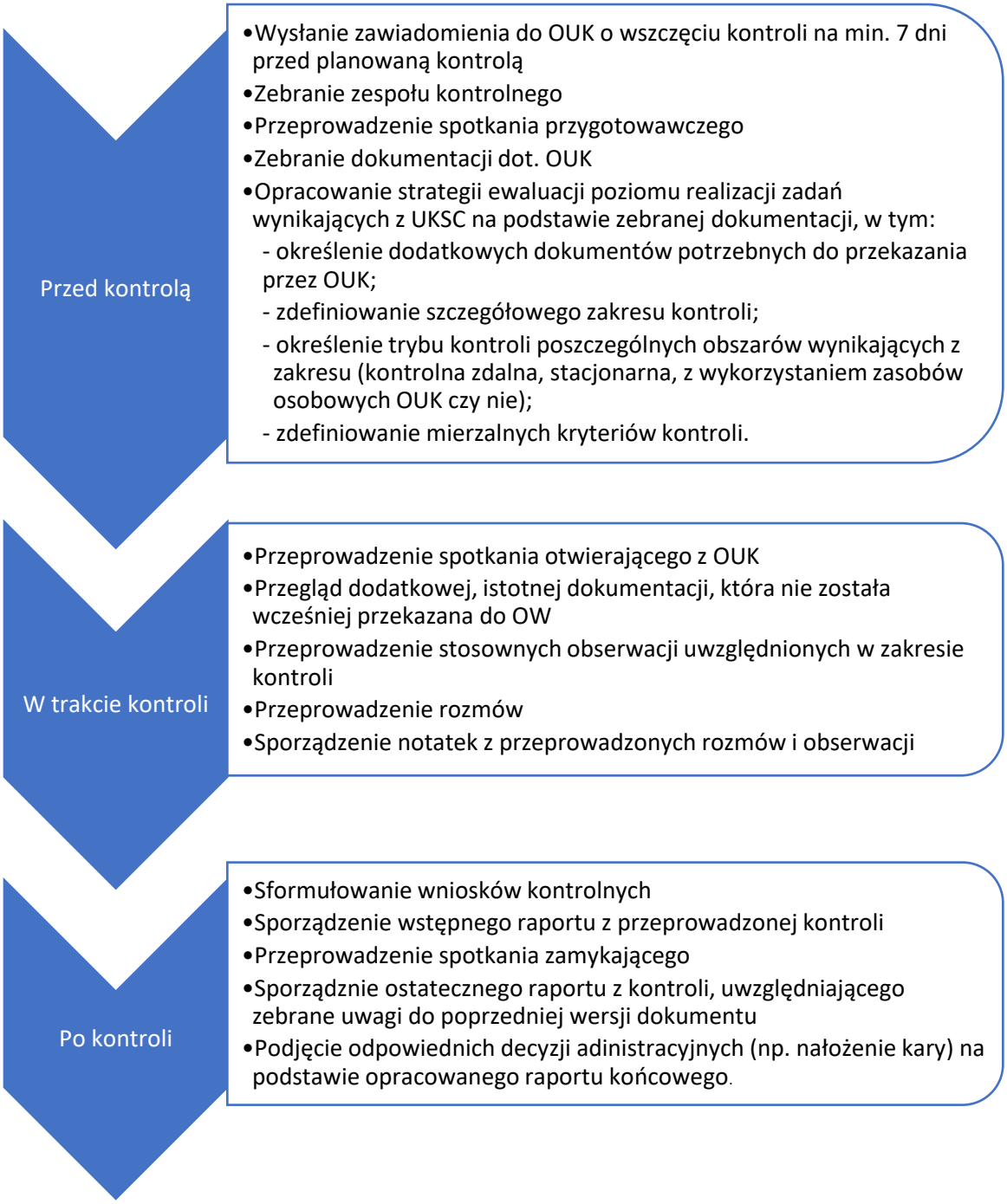
[5] *Rekomendacje Ministra Klimatu i Środowiska dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów*, wrzesień 2021 r.

gospodarczej przez przedsiębiorcę będącego OUK oraz jego innych szczegółowych obowiązków określonych w UKSC.

USTALENIE POTRZEBY PRZEPROWADZENIA KONTROLI

Na podstawie zbiorczych ocen operatorów usług kluczowych sektora energii, pod kątem realizacji wymagań z zakresu cyberbezpieczeństwa i zbudowanego rankingu, Ministerstwo Klimatu i Środowiska może wystąpić w trybie art. 43 ust. 2 UKSC do operatora usługi kluczowej o udzielenie informacji, które umożliwią ustalenie potrzeby przeprowadzania kontroli.

9. Realizacja kontroli



10. Etapy kontroli

POINFORMOWANIE PRZEDSIĘBIORCY O KONTROLI

Ministerstwo Klimatu i Środowiska ma obowiązek zawiadomić przedsiębiorcę o zamiarze wszczęcia kontroli.

Kontrolę wszczyna się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze wszczęcia kontroli. Jeżeli kontrola nie zostanie wszczęta w terminie 30 dni od dnia doręczenia zawiadomienia, wszczęcie kontroli wymaga ponownego zawiadomienia. Wzór zawiadomienia o zamiarze wszczęcia kontroli stanowi załącznik nr 3.

Zawiadomienie o zamiarze wszczęcia kontroli zawiera:

1. oznaczenie organu;
2. datę i miejsce wystawienia;
3. oznaczenie przedsiębiorcy;
4. wskazanie zakresu przedmiotowego kontroli;
5. imię, nazwisko oraz podpis osoby upoważnionej do zawiadomienia z podaniem zajmowanego stanowiska lub funkcji.

Należy mieć na uwadze, że na wniosek przedsiębiorcy kontrola może zostać wszczęta przed upływem 7 dni od dnia doręczenia zawiadomienia.

Zgodnie z art. 48 ust. 5 UPP, czynności kontrolne związane z pobieraniem próbek i dokonywaniem oględzin, w tym pojazdów, lub dokonywaniem pomiarów mogą być wykonywane przed upływem terminu 7 dni. Czynności wykonywane w tym trybie związane z pobieraniem próbek i dokonywaniem oględzin nie mogą przekraczać jednego dnia roboczego, natomiast czynności związane z dokonywaniem pomiarów nie mogą przekraczać kolejnych 24 godzin liczonych od chwili rozpoczęcia tych czynności. W tym przypadku oględziny nie mogą dotyczyć treści dokumentów. Z wykonanych czynności kontrolnych w tym trybie sporządza się protokół.

W przypadku, gdy organ kontrolujący nie dostarczy zawiadomienia o zamiarze wszczęcia kontroli, to uzasadnienie przyczyny braku zawiadomienia umieszcza się w protokole kontroli.

Zawiadomienia o zamiarze wszczęcia kontroli nie dokonuje się, w przypadku gdy:

1) kontrola ma zostać przeprowadzona na podstawie ratyfikowanej umowy międzynarodowej albo bezpośrednio stosowanych przepisów prawa Unii Europejskiej;
2) przeprowadzenie kontroli jest niezbędne dla przeciwdziałania popełnieniu przestępstwa lub wykroczenia, przeciwdziałania popełnieniu przestępstwa skarbowego lub wykroczenia skarbowego lub zabezpieczenia dowodów jego popełnienia;
3) kontrola jest przeprowadzana na podstawie przepisów ustawy z dnia 25 sierpnia 2006 r. o systemie monitorowania i kontrolowania jakości paliw (Dz.U. z 2019 r. poz. 660 i 1527 oraz z 2020 r. poz. 284);
4) przeprowadzenie kontroli jest uzasadnione bezpośrednim zagrożeniem życia, zdrowia lub środowiska;

5) kontrola jest prowadzona w toku postępowania prowadzonego na podstawie przepisów ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2020 r. poz. 1076 i 1086);
6) przeprowadzenie kontroli jest niezbędne dla przeciwdziałania naruszeniu zakazów, o których mowa w art. 44b ust. 1 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz.U. z 2020 r. poz. 2050);
7) kontrola jest prowadzona na podstawie art. 23b lub art. 23r ust. 1 ustawy z dnia 10 kwietnia 1997 r. - Prawo energetyczne (Dz.U. z 2020 r. poz. 833, 843, 1086, 1378 i 1565);
8) kontrola jest przeprowadzana na podstawie przepisów ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska (Dz.U. z 2020 r. poz. 995, 1339 i 2127) w zakresie poziomów pól elektromagnetycznych emitowanych z instalacji radiokomunikacyjnej, radionawigacyjnej lub radiolokacyjnej;
9) przedsiębiorca nie ma adresu zamieszkania lub adresu siedziby lub doręczanie pism na podane adresy było bezskuteczne lub utrudnione;
10) kontrola dotyczy przypadków określonych w art. 282c ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa;
11) kontrola jest przeprowadzana na podstawie przepisów ustawy z dnia 25 sierpnia 2006 r. o biokomponentach i biopaliwach ciekłych (Dz.U. z 2020 r. poz. 1233 i 1565);
12) kontrola jest przeprowadzana na podstawie przepisów ustawy z dnia 13 lutego 2020 r. o ochronie roślin przed agrofagami (Dz.U. poz. 424 i 695);
13) kontrola jest przeprowadzana wyłącznie w celu sprawdzenia wykonania wezwania, o którym mowa w art. 21a ust. 1, zobowiązania, o którym mowa w art. 21a ust. 2, lub weryfikacji powiadomienia, o którym mowa w art. 21a ust. 5 lub 6 UPP.

MIEJSCE KONTROLI

Kontrolę przeprowadza się w siedzibie przedsiębiorcy lub w miejscu wykonywania działalności gospodarczej oraz w godzinach pracy lub w czasie faktycznego wykonywania działalności gospodarczej przez przedsiębiorcę.

Za zgodą lub na wniosek przedsiębiorcy kontrolę przeprowadza się w miejscu przechowywania dokumentacji, innym niż siedziba lub miejsce wykonywania działalności gospodarczej, jeżeli może to usprawnić prowadzenie kontroli.

Za zgodą przedsiębiorcy kontrola lub poszczególne czynności kontrolne mogą być przeprowadzane również w siedzibie organu kontroli, a więc w MKiŚ jeżeli może to usprawnić prowadzenie kontroli. Wzór wystąpienia o wyrażenie zgody na przeprowadzenie kontroli w siedzibie Ministerstwa Klimatu i Środowiska stanowi załącznik nr 2.

Za zgodą przedsiębiorcy kontrola lub poszczególne czynności kontrolne mogą być przeprowadzone w sposób zdalny za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz.U. z 2020 r. poz. 1041) lub za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344), jeżeli może to usprawnić prowadzenie kontroli lub przemawia za tym charakter prowadzonej przez przedsiębiorcę działalności gospodarczej – załącznik nr 7.

Dokumenty oraz informacje zebrane w toku czynności wykonywanych przez organ kontroli z naruszeniem przepisów zawartych w art. 51 ust. 2-3a UPP nie stanowią dowodu w postępowaniu kontrolnym.

CZYNNOŚCI KONTROLNE

Czynności kontrolne mogą być wykonywane przez pracowników Ministerstwa Klimatu i Środowiska po okazaniu operatorowi usługi kluczowej albo osobie przez niego upoważnionej legitymacji służbowej upoważniającej do wykonywania takich czynności oraz po doręczeniu upoważnienia do przeprowadzenia kontroli. Czynności kontrolne mogą być wykonywane przez osoby niebędące pracownikami Ministerstwa Klimatu i Środowiska, jeżeli odrębne przepisy przewidują taką możliwość.

Do pracowników Ministerstwa Klimatu i Środowiska jako organu kontroli oraz osób niebędących pracownikami organu kontroli (jeżeli odrębne przepisy przewidują taką możliwość), stosuje się przepisy Kodeksu postępowania administracyjnego dotyczące wyłączenia pracownika, chyba że odrębne przepisy stanowią inaczej.

Zmiana osób upoważnionych do przeprowadzenia kontroli, zakresu przedmiotowego kontroli oraz miejsca wykonywania czynności kontrolnych wymaga każdorazowo wydania odrębnego upoważnienia. Zmiany te nie mogą prowadzić do wydłużenia przewidywanego wcześniej terminu zakończenia kontroli.

Upoważnienie, o którym mowa powyżej, zawiera w szczególności:

1) wskazanie podstawy prawnej;
2) oznaczenie organu kontroli;
3) datę i miejsce wystawienia;
4) imię i nazwisko pracownika organu kontroli uprawnionego do przeprowadzenia kontroli oraz numer jego legitymacji służbowej;
5) oznaczenie przedsiębiorcy objętego kontrolą;
6) określenie zakresu przedmiotowego kontroli;
7) wskazanie daty rozpoczęcia i przewidywanego terminu zakończenia kontroli;
8) imię, nazwisko oraz podpis osoby udzielającej upoważnienia z podaniem zajmowanego stanowiska lub funkcji;
9) pouczenie o prawach i obowiązkach przedsiębiorcy.

Dokument, który nie spełnia wymagań, o których mowa wyżej, nie stanowi podstawy do przeprowadzenia kontroli. Wzór upoważnienia stanowi załącznik nr 8.

Zakres kontroli nie może wykraczać poza zakres wskazany w upoważnieniu.

Należy dodać, że podstawową zasadą postępowania kontrolnego jest zasada prawdy obiektywnej, zgodnie z którą ustalenia dokonane podczas czynności kontrolnych powinny przedstawiać rzeczywisty obraz kontrolowanych działań. Chodzi tu przede wszystkim o bezstronne i uczciwe dokonywanie ustaleń, a także przedstawianie ich w oparciu o rzetelnie zebrany materiał dowodowy.

Czynności kontrolne wykonuje się w obecności przedsiębiorcy lub osoby przez niego upoważnionej.

Czynności kontrolne wykonuje się w sposób sprawny i możliwie niezakłócający funkcjonowania przedsiębiorcy. W przypadku gdy przedsiębiorca wskaże na piśmie, że wykonywane czynności zakłócają w sposób istotny działalność gospodarczą przedsiębiorcy, konieczność podjęcia takich czynności uzasadnia się w protokole kontroli.

11. Elementy do zweryfikowania

Bezpieczeństwo systemów informacyjnych wymaga zapewnienia bezpieczeństwa na poziomie rozwiązań organizacyjnych, w sferze technicznej (logicznej), zabezpieczeń fizycznych, a także podejścia w zakresie zarządzania zasobami ludzkimi. Wymagania w wyżej wymienionych obszarach zostały zdefiniowane w ustawie o krajowym systemie cyberbezpieczeństwa (UKSC) oraz towarzyszących jej aktach wykonawczych. Ponadto we wrześniu 2021 r. Minister Klimatu i Środowiska wydał dokument pt.: *Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów*. Rekomendacje składają się z 13 rozdziałów, tabeli poziomów dojrzałości organizacji oraz 5 załączników. W dokumencie zostały poruszone następujące kwestie:

- zarządzanie ryzykiem,
- zarządzanie stroną trzecią,
- cykl życia systemów informacyjnych,
- bezpieczeństwo osobowe,
- podnoszenie świadomości i szkolenia,
- audyty bezpieczeństwa systemów informacyjnych,
- zachowanie ciągłości działania i odbudowa,
- bezpieczeństwo fizyczne,
- bezpieczeństwo sieci łączności elektronicznej,
- bezpieczeństwo systemów informacyjnych,
- wytyczne sektorowe dotyczące zgłaszania incydentów.

Głównym celem opracowania rekomendacji sektorowych było stworzenie zbioru szczegółowych wytycznych wspomagających realizację wymagań prawnych i regulacyjnych z zakresu cyberbezpieczeństwa w sektorze energetycznym, określonych w przepisach prawa, z uwzględnieniem specyfiki sektora związanej z dominacją przemysłowych systemów sterowania.

W toku kontroli bezpieczeństwa systemów informacyjnych u operatora usługi kluczowej weryfikowane są zabezpieczenia dostępu do systemu informacyjnego. Ocena zarządzania cyberbezpieczeństwa operatora usługi kluczowej odbywa się poprzez weryfikację głównych elementów organizacji cyberbezpieczeństwa na poziomie podmiotu zobowiązanego. Dodatkowe obszary zainteresowania ze strony Ministerstwa Klimatu i Środowiska to proces zarządzania ryzykiem, wyniki oceny i postępowania z ryzykiem, konstrukcja danej kategorii zabezpieczenia, a także sposób zarządzania incydentem w ramach podmiotu zobowiązanego. Dowodami potwierdzającymi prawidłowe funkcjonowanie systemu, jego zabezpieczenie oraz odpowiedzialności są najczęściej określone w ramach polityk i procedur związanych z cyberbezpieczeństwem, co również jest weryfikowane podczas kontroli. Kontrolujący weryfikują również aktualność dokumentacji związanej z cyberbezpieczeństwem. Ważną kategorią zabezpieczeń jest też podnoszenie kompetencji z zakresu cyberbezpieczeństwa, dlatego kontrolowane są tego typu działania w ramach danej organizacji, m.in. poprzez wywiady z pracownikami nt. poziomu świadomości w zakresie zagadnień cyberbezpieczeństwa.

W załączniku nr 1 do niniejszego podręcznika zostały wylistowane wymagania wskazane w UKSC wraz z przykładami dokumentacji potwierdzającymi, że dany warunek został spełniony przez operatora usługi kluczowej. W kolejnych podpunktach zostały opisane bardziej szczegółowe aspekty rozwiązań organizacyjnych, w sferze technicznej (logicznej), zabezpieczeń fizycznych, a także podejścia w zakresie zarządzania zasobami ludzkimi.

PODEJŚCIE DO ZARZĄDZANIA I ORGANIZACJI CYBERBEZPIECZEŃSTWA

Punkt ten odnosi się to do stosowania środków cyberbezpieczeństwa w realizacji polityki bezpieczeństwa teleinformatycznego przez podmiot zobowiązany.

Kryteria obejmują:

1) Istnienie zatwierdzonej przez kierownictwo Polityki Bezpieczeństwa Informacji, bądź Polityki Cyberbezpieczeństwa lub innego równoważnego dokumentu;
2) Istnienie ustrukturyzowanego, sformalizowanego, udokumentowanego zestawu procedur i procesów dotyczących cyberbezpieczeństwa;
3) Wdrożone procesy umożliwiają ciągły przegląd i doskonalenie, m.in. przeglądy okresowe, audyty, przejrzyste procedury konserwacji, samooceny itp.;
4) Procesy są proaktywne w największym możliwym stopniu i nie są reaktywne.

Elementem udanego zarządzania cyberbezpieczeństwem jest też akceptacja Polityki Bezpieczeństwa Informacji, bądź Polityki Cyberbezpieczeństwa lub innego równoważnego dokumentu na wszystkich poziomach zarządzania (kierownictwo, zarząd, dyrekcja departamentu odpowiedzialnego za bezpieczeństwo teleinformatyczne) oraz jej realizacja w praktyce. Kryteria obejmują:

1) Zaangażowanie kierownictwa jest widoczne na wszystkich poziomach;
2) Cele cyberbezpieczeństwa są jasno określone;
3) Określono jednoznaczne role i obowiązki, aby zapewnić cyberbezpieczeństwo organizacji i kluczowych procesów biznesowych;
4) Role i obowiązki:
    a. obejmują wszystkie domeny funkcjonalne;
    b. są ustalane w oparciu o skoordynowane podejście pomiędzy odpowiednimi domenami funkcjonalnymi;
    c. zapewniają odpowiednią organizację, w tym ustalane konkretne funkcje dla całej organizacji, m.in. CSO (ang. *Computer Security Officer*), etc.
5) Kierownictwo zapewnia dostęp do odpowiednich zasobów (ludzkich, finansowych, alokacji czasu, umiejętności itp.);
6) Procesy zarządzania obejmują ocenę wewnętrzną i środki zapewnienia jakości;
7) Zapewniona jest zgodność z ramami regulacyjnymi, w tym z UKSC.

Art. 9 UKSC wskazuje następujące zadania operatora usługi kluczowej:

1) wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
2) przekazuje organowi właściwemu do spraw cyberbezpieczeństwa dane, o których mowa w art. 7 ust. 2 pkt 8 (informację określającą, w których państwach członkowskich Unii Europejskiej podmiot został uznany za operatora usługi kluczowej) i 9 (datę zakończenia świadczenia usługi kluczowej), nie później niż w terminie 3 miesięcy od zmiany tych danych.

Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa dane osoby, o której mowa w powyżej, zawierające imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych - w terminie 14 dni od dnia ich zmiany.

Natomiast w zakresie postępowania z dokumentacją operator usługi kluczowej ma wskazane następujące obowiązki:

1) opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
2) ustanawia nadzór nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zapewniającą:
    a. dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami;
    b. ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności;
    c. oznaczanie kolejnych wersji dokumentów, umożliwiające określenie zmian dokonanych w tych dokumentach.

Operator usługi kluczowej przechowuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej.

WYJĄTEK IK - Jeżeli OUK jest jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, który posiada zatwierdzony plan ochrony infrastruktury krytycznej uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, nie ma obowiązku opracowania dokumentacji, o której mowa powyżej.

STRUKTURY OPERATORA USŁUGI KLUCZOWEJ ODPOWIEDZIALNE ZA CYBERBEZPIECZEŃSTWO

OUK powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.

Operator usługi kluczowej informuje Ministerstwo Klimatu i Środowiska i właściwy CSIRT poziomu krajowego oraz sektorowy zespół cyberbezpieczeństwa o podmiocie, z którym została zawarta umowa o świadczenie usług z zakresu cyberbezpieczeństwa, danych kontaktowych tego podmiotu, zakresie świadczonej usługi oraz o rozwiązaniu umowy w terminie 14 dni od dnia zawarcia lub rozwiązania umowy. Powyższe informacje są weryfikowane także podczas kontroli.

W przypadku, gdy zadania z zakresu cyberbezpieczeństwa są realizowane przez wewnętrzne struktury powołane przez operatora usługi kluczowej i obejmują:

- wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej (SZBI),

- udostępnianie użytkownikowi usługi kluczowej wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową,
- zarządzanie dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej,
- zarządzanie incydentami, w tym zgłaszanie incydentów poważnych do CSIRT poziomu krajowego,
- przekazywanie do CSIRT poziomu krajowego informacji o innych incydentach; zagrożeniach cyberbezpieczeństwa, dotyczących szacowania ryzyka, podatnościach, wykorzystywanych technologiach.

Ww. struktury są obowiązane spełniać wymagania organizacyjne i techniczne, określone w rozporządzeniu Ministra Cyfryzacji z 4 grudnia 2019 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*. Ww. wymagania zostały opisane w załączniku nr 1 do niniejszego podręcznika.

PODEJŚCIE DO ZABEZPIECZEŃ TECHNICZNYCH

Rozwiązania techniczne obejmują swoim zakresem każde przypadki zastosowania urządzenia, oprogramowania i konkretnej technologii w sferze specyfiki systemów informacyjnych operatorów usług kluczowych, mogących realizować funkcje operacyjne, biznesowe, bezpieczeństwa (*safety*), ochrony fizycznej, reagowania kryzysowego. Kluczowym elementem w obszarze technologicznym jest bezpieczeństwo oprogramowania, definiowane jako zapobieganie występowaniu błędów, które mogą pozwalać na przejęcie kontroli nad aplikacją, urządzeniem bądź systemem. Innym przykładem jest odporność systemu transmisyjnego na zakłócenia, czyli zabezpieczenie transmisji danych przed przechwyceniem lub zniekształceniem informacji. Innym rodzajem zabezpieczenia jest wprowadzanie monitorowania, który pracownik ma dostęp do poszczególnych kategorii informacji. Dzięki takiemu rozwiązaniu, w przypadku wycieku danych, organizacja może określić kto jest odpowiedzialny za dany wyciek oraz oszacować skalę zjawiska. Powyższe elementy zabezpieczeń technicznych są weryfikowane są w toku działalności kontrolnej.

Przykładami ocenianych zabezpieczeń technicznych są następujące rozwiązania:

1) IPS – Intrusion Prevention System

System IPS (ang. Intrusion Prevention System – IPS), czyli system zapobiegający włamaniom to rodzaj urządzenia sieciowego wykrywającego i blokującego ataki na systemy informacyjne. Działanie urządzenia polega na monitorowaniu kluczowych elementów systemu w poszukiwaniu niepożądanych zachowań i zdarzeń, takich jak robaki internetowe, trojany, oprogramowanie typu *spyware* lub *malware* oraz ich powstrzymywaniu. IPS może spowodować odłączenie sieci komputerowej lub przerwanie sesji użytkownika poprzez zablokowanie określonemu numerowi IP dostępu do zasobu lub usługi, niektóre rozwiązania pozwalają również na rekonfigurację „zapory sieciowej" (ang. firewall) lub routera.

2) NGFW – Next Generation Firewall

„Zapora sieciowa" (ang. firewall) to rozwiązanie sprzętowe, obejmujące routery, serwery i oprogramowanie, ograniczające przepływ pakietów danych pomiędzy segmentami sieci komputerowej zgodnie z określoną polityką bezpieczeństwa. W przypadku Next Genaration Firewall tradycyjna technologia „zapory sieciowej" jest poszerzona o inne urządzenia sieciowe z funkcją filtrowania pakietów danych, w tym dokonujących pakietowej inspekcji danych (ang. DPI – deep packet inspection) oraz o systemy zapobiegające włamaniom IPS. Celem implementacji narzędzi klasy NGFW jest realizacja inspekcji pakietów danych na większej liczbie warstw modelu OSI[6].

3) WAF - Web Application Firewall

Technologia aplikacyjnej „zapory sieciowej" to technologia umożliwiająca przepływy informacji między systemami komputerowymi, ale bez bezpośredniej możliwości wymiany pakietów danych. Technologia ta pozwala ograniczyć ryzyko związane z wymianą pakietów danych pomiędzy systemami wewnętrznymi i zewnętrznymi i aplikacji hostowanych w sieci korporacyjnej. Aplikacyjna „zapora sieciowa" to urządzenie lub oprogramowanie umiejscowione na "utwardzonym" systemie operacyjnym np. Windows lub UNIX, funkcjonującą w aplikacyjnej warstwie modelu OSI. WAF analizuje przepływy informacji w oparciu o serwery proxy (serwery pośredniczące), obsługujące żądania klientów poprzez przesyłanie żądań do innych serwerów z własnym adresem sieciowym dla każdej usługi (np. FTP, Telnet czy http).

4) DLP – Data Leak Prevention

Oprogramowanie tego typu służy do ochrony danych przed wyciekiem, dotyczy to zarówno wycieków przypadkowych, wynikających na przykład z nieostrożności pracowników oraz działań celowych. Większość rozwiązań klasy DLP ułatwia lokalizację i katalogowanie informacji wrażliwych, monitoring i kontrolę przepływu informacji poprzez sieci korporacyjne oraz urządzenia końcowe. W tym celu wykorzystywane są tzw. „crawlery"[7] przeszukujące zbiory danych, urządzenia sieciowe monitorujące ruch sieciowy, w tym dokonujące pakietowej inspekcji danych (ang. DPI – Deep Packet Inspection), a także urządzenia monitorujące działania użytkowników końcowych na stacjach roboczych. Szczególnie istotne w przypadku rozwiązań klasy DLP jest przeprowadzenie szacowania bezpieczeństwa informacji, określenie wartości przetwarzanych informacji, a także ustanowienie polityk, reguł wykonywania operacji przez oprogramowanie i komponenty sprzętowe systemu klasy DLP.

5) SIEM – Security Information and Event Management

System SIEM to oprogramowanie przeznaczone do agregowania i analizowania znacznej liczby danych i informacji, zarówno z urządzeń końcowych, jak i z narzędzi do monitorowania sieci, takich jak „zapory sieciowe" czy systemy IPS. Systemy SIEM w sposób automatyczny agregują i korelują dane i logi związane ze zdarzeniami cyberbezpieczeństwa, w powiązaniu z analizą danych historycznych. Korelacja zdarzeń oznacza, że system SIEM umożliwia stworzenie jednego zdarzenia mającego charakter incydentu cyberbezpieczeństwa. Korelacja oparta na regułach pozwala określić wzorzec zdarzeń cyberbezpieczeństwa, natomiast korelacja oparta na statystykach pozwala zdefiniować poziom zagrożeń dla aktywów informacyjnych. Informacje z systemów mogą być wykorzystywane przez

[6] Model referencyjny opisujący strukturę komunikacji w sieci komputerowej.
[7] Program zbierający informacje o strukturze danych, stronach i treściach.

wewnętrzne zespoły typu CSIRT czy operacyjne centra bezpieczeństwa (ang. SOC – Security Operations Center).

6) SOAR – Security Orchestration, Automation and Response

SOAR to nowa, zyskująca coraz bardziej na znaczeniu technologia w bezpieczeństwie IT, szczególnie interesująca dla organizacji dysponujących własnym SOC (Security Operations Centre) lub aktywnie użytkujących system klasy SIEM. SOAR jest nową klasą systemów IT Sec, których zadaniem jest skuteczniejsze zarządzanie zdarzeniami cyberbezpieczeństwa występującymi w systemach IT/OT organizacji. Ich funkcjonalność sprowadza się zasadniczo do trzech obszarów: automatyzacja procesów reagowania na incydenty w oparciu o playbooki, automatyczne wzbogacanie zdarzeń cyberbezpieczeństwa o dodatkowe informacje w oparciu o różnorodne integracje oraz strukturyzacja procesów w oparciu o role i tickety.[8]

7) EDR – Endpoint Detection and Response

EDR to rodzaj narzędzia informatycznego monitorującego wykorzystywane w organizacji i jej sieci korporacyjnej urządzenia końcowe (np. telefon komórkowy, laptop, stacja robocza, urządzenie Internetu Rzeczy) celem zapobiegania zagrożeniom cyberbezpieczeństwa. Technologia EDR służy do identyfikowania podejrzanych zachowań i zaawansowanych trwałych zagrożeń cyberbezpieczeństwa na punktach końcowych w środowisku informatycznym oraz do odpowiedniego ostrzegania administratorów. Jest to realizowane poprzez zbieranie i agregowanie danych z punktów końcowych i innych źródeł. Te dane mogą, ale nie muszą, zostać wzbogacone o dodatkową analizę w chmurze. Rozwiązania EDR to przede wszystkim narzędzie ostrzegania, a nie warstwa ochrony, ale funkcje mogą być łączone w zależności od dostawcy. Dane mogą być przechowywane w scentralizowanej bazie danych lub przekazywane do narzędzia SIEM.

8) XDR – Extended Detection and Response

Rozszerzone możliwości wykrywania zagrożeń cyberbezpieczeństwa i reagowania na nie, określane skrótem XDR, to narzędzie w modelu Software-as-A-Service, które oferuje kompleksowe, zoptymalizowane zabezpieczenia, integrując produkty zabezpieczające oraz dane w uproszczone rozwiązania. W przeciwieństwie do systemów takich jak wykrywanie i reagowanie w punktach końcowych (EDR), system XDR rozszerza zakres zabezpieczeń, integrując ochronę z szerszą gamą produktów, w tym z punktami końcowymi organizacji, serwerami, aplikacjami w chmurze, pocztą e-mail. Dzięki temu system XDR łączy zapobieganie, wykrywanie, badanie i reagowanie, zapewniając widoczność, analizę, skorelowane alerty o incydentach i automatyczne reakcje w celu poprawy bezpieczeństwa danych i zwalczania zagrożeń cyberbezpieczeństwa[9].

Ponadto, w obszarze technologicznym w sektorze energetycznym w toku kontroli należy zweryfikować i uwzględnić takie czynniki jak odporność na warunki pracy i wpływ środowiska, a także niezawodność funkcjonowania w cyklu życia urządzenia, czyli czas do pierwszej awarii. Organizacja powinna dążyć do unifikacji i standaryzacji architektury rozwiązań, również poprzez modernizację lub wdrażanie nowych systemów w miejsce starszych, już wykorzystywanych. Pożądanym rozwiązaniem jest stopniowe wycofanie systemów informacyjnych, które z racji swojego wieku i długiej eksploatacji nie są objęte

[8] https://mediarecovery.pl/soar-czyli-wyzszy-poziom-soc/
[9] https://www.microsoft.com/pl-pl/security/business/security-101/what-is-xdr

procesem aktualizacji, dostarczania poprawek bezpieczeństwa oraz tych, które są niekompatybilne z innymi systemami odpowiadającymi za bezpieczeństwo, mając na uwadze możliwe korzyści i straty wynikające z planowanej modernizacji. Powinno się także stosować uzupełniające środki bezpieczeństwa w starszych systemach, m.in. poprzez zapewnienie dodatkowych środków bezpieczeństwa fizycznego, takich jak środki ochrony przeciwpożarowej, systemy sygnalizacji włamania i napadu, kontroli dostępu, ochrony obwodowej, czy poprzez przeniesienie rozliczalności dostępu. Te okoliczności są również weryfikowane w toku kontroli.

ZARZĄDZANIE ZAGROŻENIAMI CYBERBEZPIECZEŃSTWA, INCYDENTAMI I ICH KONSEKWENCJAMI

Operator usługi kluczowej powinien zdefiniować, czym jest zagrożenie cyberbezpieczeństwa. Zagrożenie powinno być stale monitorowane, przeglądane i oceniane pod kątem wszelkich zmian, które mogą mieć wpływ na cyberbezpieczeństwo organizacji i świadczonych przez nią usług kluczowych.

Kryteria i pytania obejmują:

1) Organizacja posiada dojrzały proces zarządzania, który obejmuje analizę i zarządzanie zagrożeniami cyberbezpieczeństwa, podatnościami i potencjalnymi ich konsekwencjami.
2) Jakie metody zarządzania zagrożeniami cyberbezpieczeństwa są stosowane?
3) Jaki jest zakres analizy zagrożeń (np. organizacja, część organizacji, system itp.)?
4) Sposób przeprowadzenia, udokumentowania i wykorzystania analizy w połączeniu z podstawowymi mechanizmami kontroli bezpieczeństwa.
5) Potencjalne zagrożenia zostały zidentyfikowane i ocenione. Ten proces powinien być realizowany na bieżąco, a także powinien przewidywać nowe, potencjalne zagrożenia w przyszłości.
6) Ww. oceny obejmują analizę potencjalnych konsekwencji związanych z cyberatakami.
7) W odniesieniu do sposobu przeprowadzania ocen zagrożeń cyberbezpieczeństwa, jak często występują regularne przeglądy i aktualizacje?
8) Czy w ramach procesu reagowania na incydenty są uwzględnione procesy mitygacji, odzyskiwania i zachowania ciągłości świadczenia usług kluczowych?

Obowiązkiem operatora usługi kluczowej jest wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, który zapewnia (art. 8 UKSC):

1) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
2) zarządzanie incydentami;
3) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
    a. stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
    b. dbałość o aktualizację oprogramowania,
    c. ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
    d. niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;

OUK (art. 11 UKSC):

1) zapewnia obsługę incydentu

2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań;
3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny;
4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

Dodatkowe zadania będą nałożone na operatora usługi kluczowej, gdy powstanie sektorowy zespół cyberbezpieczeństwa (art. 11 ust. 3).

Zgłoszenie incydentu poważnego do CSIRT poziomu krajowego powinno zawierać określone elementy – to również należy zbadać podczas kontroli, czy przekazywane zgłoszenia były kompletne (art. 12 UKSC – wymagania co do zgłaszania incydentów).

ZARZĄDZANIE RYZYKIEM

Operator usługi kluczowej musi zapewnić, że organizacja jest w stanie ustalić i utrzymać ryzyko naruszenia cyberbezpieczeństwa na akceptowalnym poziomie poprzez zarządzanie ryzykiem wystąpienia incydentu. Procesy związane z bezpieczeństwem i zachowaniem ciągłości świadczenia usługi kluczowej powinny uwzględniać stosowanie podstawowych zasad bezpieczeństwa, w tym zachowanie bezpieczeństwa zasobów organizacji przed zdarzeniami związanymi z bezpieczeństwem fizycznym zgodnie z poziomem konsekwencji lub wpływu, jaki te zdarzenia mogą spowodować.

Kryteria i pytania obejmują:
1) Poziomy bezpieczeństwa zostały ustalone zgodnie z jasnymi procesami lub regułami (np. w oparciu o bezpieczeństwo, analizę potencjalnych konsekwencji, itp.). Czy te procesy lub zasady są faktycznie stosowane?
2) W jaki sposób wdrażana jest ochrona komponentów i systemów teleinformatycznych (IT i OT)?
3) Jak oceny ryzyka wpływają na podejście stopniowe (ang. *graded approach*)?
4) Czy podejście stopniowe obejmuje wszystkie pozycje zidentyfikowane w ocenie ryzyka?

Obowiązkiem operatora usługi kluczowej jest wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, który zapewnia (art. 8 UKSC):
1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
    a. utrzymanie i bezpieczną eksploatację systemu informacyjnego,
    b. bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
    c. bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
    d. wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
    e. objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

PODNOSZENIE KOMPETENCJI Z ZAKRESU CYBERBEZPIECZEŃSTWA

W przypadku ryzyka bezpieczeństwa systemów informacyjnych występującego w organizacji, gdzie nie można zastosować zabezpieczeń technicznych ani wykorzystać narzędzi testowania, zasadne jest przygotowanie programu szkoleń i działań uświadamiających pracowników i specjalistów. Podmiot wyznaczony jako operator usługi kluczowej powinien zagwarantować podobny poziom wiedzy bazowej wszystkich pracowników swojej organizacji w zakresie tematyki cyberbezpieczeństwa, a także prowadzić cykliczne szkolenia dla wszystkich zatrudnionych osób, aby regularnie budować świadomość cyberbezpieczeństwa w ramach swojej organizacji. Organizacja powinna również zidentyfikować różne grupy docelowe szkoleń – od podstawowych użytkowników systemów po osoby bezpośrednio zajmujące się bezpieczeństwem sieci i systemów IT i OT. Zakres szkoleniowy powinien być odpowiednio dopasowany w zależności od kompetencji potrzebnych do realizacji zadań na danym stanowisku.

Pracownicy, których zakres obowiązków obejmuje zaawansowaną wiedzę techniczną z zakresu cyberbezpieczeństwa, powinni mieć zapewniony dostęp do cyklicznych szkoleń i odpowiednich ścieżek rozwoju. W tym celu uzasadnione jest opracowanie odpowiedniego programu szkoleń dla specjalistów zajmujących się cyberbezpieczeństwem, aby poziom ich wiedzy był na wysokim poziomie, co będzie gwarancją lepszego przygotowania na wystąpienie potencjalnego cyberataku i odpowiedniej reakcji.

Organizacje winny brać aktywny udział w organizowanych krajowych ćwiczeniach cyberbezpieczeństwa, jak również, w ramach możliwości, w tych organizowanych na poziomie międzynarodowym.

Ponadto art. 9 UKSC wskazuje następujące zadania operatora usługi kluczowej, który ma zapewniać użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej.

Wszystkie powyższe kwestie są weryfikowane przez Ministerstwo Klimatu i Środowiska w toku działań kontrolnych.

AUDYT BEZPIECZEŃSTWA SYSTEMU INFORMACYJNEGO I TERMINY REALIZACJI OBOWIĄZKÓW USTAWOWYCH

Operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Na podstawie zebranych dokumentów i dowodów audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je operatorowi usługi kluczowej wraz z dokumentacją z przeprowadzonego audytu.

Operator usługi kluczowej, u którego w danym roku w stosunku do systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej został przeprowadzony przez osoby spełniające warunki określone w ust. 2 pkt 2 audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. *o informatyzacji*

działalności podmiotów realizujących zadania publiczne, nie ma obowiązku przeprowadzania audytu przez 2 lata. Powyższe aspekty mogą być weryfikowane w toku działalności kontrolnej.

Podczas kontroli organ kontrolujący powinien również zweryfikować kwestie dochowania terminów wskazanych w UKSC. Operator usługi kluczowej realizuje obowiązki określone w:

1) art. 8 pkt 1 i 4 (zarządzanie incydentami) , art. 9 (osoba odpowiedzialna w KSC, materiały związane z cyberbezpieczeństwem), art. 11 ust. 1-3 (obsługa incydentu), art. 12 (zgłaszanie incydentów) i art. 14 ust. 1 (struktury odpowiedzialne za cyberbezpieczeństwo) - w terminie 3 miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej;
2) art. 8 pkt 2, 3, 5 i 6 (wdrożenie zabezpieczeń, zarządzanie zagrożeniami cyberbezpieczeństwa) oraz art. 10 ust. 1-3 (dokumentacja dotycząca systemu informacyjnego) - w terminie 6 miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej;

12. Metodyka doboru próby do kontroli

OCENA ZGODNOŚCI

Proces zbierania informacji obejmuje analizowanie dokumentów i zapisów dostarczonych przez operatorów usług kluczowych. Celem tego jest:

- Ocena zgodności poziomu cyberbezpieczeństwa z wewnętrznymi procedurami;
- Ocena zgodności z UKSC, przepisami krajowymi, wymogami regulacyjnymi oraz rekomendacjami (Ocena zgodności z kryteriami nieobowiązkowymi ma na celu pomóc podmiotowi nadzorującemu lepiej ocenić dojrzałość organizacji);
- Ocena zgodności z odpowiednimi wytycznymi międzynarodowymi, takimi jak wytyczne ENISA, NISD, czy inne standardy, takie jak ISO27001, ISO22301, czy IEC62443;
- Ocena istotności aktywów w kontekście aktualnego środowiska zagrożeń;
- Identyfikacja dodatkowych procesów i systemów niezbędnych do szczegółowej oceny w organizacji.

Dokumenty i zapisy to między innymi:

- polityki;
- procedury;
- regulacje wewnętrzne;
- sprawozdania z poprzednich ocen (zewnętrzne, audyt wewnętrzny, itp.);
- strony internetowe (Intranet i Internet)
- listy kontroli dostępu;
- pliki konfiguracyjne;
- diagramy sieciowe;
- schematy obiektów;
- dzienniki operacyjne;
- zestawy reguł (np. zapory firewall, IDS, routery, itp.).

Zgodnie z rozporządzeniem Rady Ministrów z dnia 16 października 2018 r. *w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej* dokumentacja dotycząca cyberbezpieczeństwa dzieli się na 2 rodzaje:

1. dokumentacja normatywna – w ramach tej dokumentacji wymienia się:
    a. dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami normy PN-EN ISO/IEC 27001;
    b. dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa, dotycząca:
        i. charakterystyki usługi kluczowej oraz infrastruktury,
        ii. szacowania ryzyka dla obiektów infrastruktury,
        iii. oceny aktualnego stanu ochrony infrastruktury (plan postępowania z ryzykiem),
        iv. opisu zabezpieczeń technicznych obiektów infrastruktury,
        v. zasad organizacji i wykonywania ochrony fizycznej infrastruktury,
        vi. danych o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2017 r. poz. 2213 oraz z 2018 r. poz. 138, 650, 1629 i 1669), chroniącej infrastrukturę, jeśli taka formacja występuje;
    c. dokumentacja systemu zarządzania ciągłością działania usługi kluczowej wytworzona zgodnie z wymaganiami normy PN-EN ISO 22301;
    d. dokumentacja techniczna systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
    e. dokumentacja wynikająca ze specyfiki świadczonej usługi kluczowej w danym sektorze lub podsektorze.
2. dokumentacja operacyjna – w ramach tej dokumentacji wymienia się:
    a. dokumentacja dotycząca procedur oraz instrukcji wynikających z dokumentacji normatywnej;
    b. opisy sposobów dokumentowania wykonania czynności w ramach ustalonych procedur;
    c. dokumentacja poświadczająca każdorazowe wykonanie procedury.

13. Techniki gromadzenia dowodów kontroli

POSTĘPOWANIE DOWODOWE

Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli. Ustawodawca w tym aspekcie dał możliwość wyboru w jakiej formie będzie zbierać dowody. Mogą one mieć postać:

- dokumentów,
- przedmiotów,
- oględzin,
- ustnych lub pisemnych wyjaśnień oraz oświadczeń.

UKSC nie dokonuje hierarchizacji dowodów, więc każdy z nich jest równy i ma taki sam wpływ na ustalenie stanu faktycznego. Osoba kontrolująca powinna na podstawie zebranych materiałów przeprowadzić z nich dowód. Należy dodać, że z racji tego, że katalog dowodów wskazany w ustawie jest otwarty, to można również przeprowadzić dowód z innych zebranych materiałów nienazwanych,

tzn. zgodnie z wyrokiem Sądu Apelacyjnego w Poznaniu z 20 lipca 2017 r. dowodami mogą być, obok dokumentów, oględzin, opinii biegłego, także zdjęcia znalezione w Internecie.

Dowód rzeczowy podczas kontroli nie jest tak szeroko wykorzystywany jak dowód z dokumentacji. Zaletą dowodu rzeczowego jest jego trwałość, co powoduje, że zebrane na ich podstawie informacje nie ulegają deformacjom w zakresie postrzegania, zapamiętania czy potrzeby odtworzenia w późniejszym czasie. Rodzajem dowodu rzeczowego może być każdy przedmiot, którego cechy mogą dostarczyć informacji dla osoby kontrolera. Aby przeprowadzić dowód z dowodu rzeczowego należy dokonać oględzin, dzięki którym uzyskuje się informacje o właściwościach zewnętrznych i wewnętrznych danego przedmiotu. Celem oględzin jest zidentyfikowanie wskazanych wyżej właściwości. Ryzykiem jakie niesie za sobą dokonanie oględzin może być zamieszczenie danych ustalonych na podstawie dokumentów, opinii, oświadczeń czy wyjaśnień, a nie bezpośrednio z oględzin danego przedmiotu.

Podmiot kontrolujący ma możliwość zweryfikowania prawdziwości oświadczeń składanych przez podmiot kontrolowany, poprzez wezwanie strony do przekazania danych pozwalających na weryfikację ich prawdziwości. Wzór dokumentu stanowi załącznik nr 4.

UPRAWNIENIA PODMIOTU KONTROLOWANEGO

Do zbioru dowodów należy również dodać oświadczenia przedstawicieli podmiotu kontrolowanego. Należy pamiętać, że katalog podmiotowy jest tu dosyć szeroki, ponieważ oświadczenia mogą składać pracownicy, a także byli pracownicy jednostki kontrolowanej, a także każda osoba, która może dostarczyć kontrolerowi informacji dotyczących zakresu kontroli.

Na podstawie powyższego należy również wskazać różnicę pomiędzy dowodem z wyjaśnień a dowodem z oświadczeń. Podstawową różnicą jest fakt, że inicjatorem wyjaśnień jest kontroler, a oświadczenia – osoba składająca dane oświadczenie.

14. Zakończenie kontroli

PROTOKÓŁ KONTROLI

Zgodnie z obowiązującymi regulacjami, ustalenia dokonane podczas działań kontrolnych mają zostać udokumentowane w postaci protokołu kontroli, który podlega pod procedurę odwoławczą. Dokument ten powinien zawierać przebieg przeprowadzonej kontroli. UKSC jednoznacznie określa elementy takiego protokołu kontroli. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami przedstawia przebieg przeprowadzonej kontroli w protokole kontroli.

Protokół kontroli zawiera (Wzór protokołu stanowi załącznik 10):

1. wskazanie nazwy albo imienia i nazwiska oraz adresu podmiotu kontrolowanego;
2. imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
3. imię i nazwisko, stanowisko oraz numer upoważnienia osoby prowadzącej czynności kontrolne. Zarówno w przypadku, gdy kontrola jest prowadzona jednoosobowo, jak również przez zespół kontrolerów w protokole wymienia się wszystkie osoby prowadzące kontrolę;

4. datę rozpoczęcia i zakończenia czynności kontrolnych;
5. określenie przedmiotu i zakresu kontroli - przedmiot kontroli odnosi się do zagadnień podlegających sprawdzeniu, natomiast zakres odnosi się do okresu, w ramach którego zagadnienia będą oceniane;
6. opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
7. wyszczególnienie załączników.

W powyższym punkcie 6 ustawodawca wskazał, że należy w protokole wskazać informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości – elementy te stanowią tzw. fakt kontrolny. Opis stanu faktycznego składa się z faktów kontrolnych, które posiadają następujące elementy: obowiązująca norma prawna, działania odbiegające od normy lub zaniechania, przyczyny takiego stanu rzeczy oraz skutki odstępstwa od normy prawnej, a także ewentualnie ustalenie osób odpowiedzialnych[10]. Fakt kontrolny musi być udowodniony, czyli musi mieć odzwierciedlenie w zebranych dowodach podczas postępowania kontrolnego. Podstawowym obowiązkiem kontrolera jest ustalenie co się stało (zakres nieprawidłowości), dlaczego tak się stało (przyczyny wystąpienia nieprawidłowości), a także określić jakie skutki ta nieprawidłowość spowodowała, czyli co z tego wynika.

Po sporządzeniu protokołu kontroli zostaje on podpisany przez osobę/osoby prowadzące czynności kontrolne oraz osoby reprezentujące podmiot kontrolowany. Przed podpisaniem protokołu podmiot kontrolowany może, w terminie 7 dni od dnia przedstawienia mu go do podpisu, złożyć pisemne zastrzeżenia do tego protokołu.

W razie zgłoszenia zastrzeżeń osoba prowadząca czynności kontrolne dokonuje ich analizy i w razie potrzeby podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu. W razie nieuwzględnienia zastrzeżeń w całości lub w części osoba prowadząca czynności kontrolne informuje podmiot kontrolowany na piśmie.

W sytuacji, gdy osoby reprezentujące podmiot kontrolowany odmówią podpisania protokołu, to wówczas osoba prowadząca czynności kontrolne czyni w protokole wzmiankę zawierającą informację o odmowie podpisania protokołu oraz datę jej dokonania.

Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej doręcza się go podmiotowi kontrolowanemu.

ZALECENIA POKONTROLNE

Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ Ministerstwo Klimatu i Środowiska uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany,

[10] Red. prof. dr hab. W.Kitler, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, 2019.

przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości. Jeżeli Ministerstwo uzna, że nie doszło do naruszenia przepisów ustawy, wówczas nie przekazuje zaleceń pokontrolnych.

Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

Podmiot kontrolowany, w wyznaczonym terminie, informuje Ministerstwo Klimatu i Środowiska o sposobie wykonania zaleceń.

Jeżeli w wyniku kontroli Ministerstwo Klimatu i Środowiska stwierdzi, że operator usługi kluczowej narusza przepisy ustawy poprzez:

1) nie przeprowadzenie systematycznego szacowania ryzyka lub nie zarządzanie ryzykiem wystąpienia incydentu, o których mowa w art. 8 pkt 1 UKSC;
2) nie wdrożenie środków technicznych i organizacyjnych uwzględniających wymagania, o których mowa w art. 8 pkt 2 lit. a-e UKSC;
3) nie stosowanie środków, o których mowa w art. 8 pkt 5 lit. a-d UKSC;
4) nie wyznaczenie osoby, o której mowa w art. 9 ust. 1 pkt 1 UKSC;
5) nie wykonanie obowiązków, o których mowa w art. 10 ust. 1 UKSC;
6) nie wykonanie obowiązku, o którym mowa w art. 11 ust. 1 pkt 1 UKSC;
7) nie wykonanie obowiązku, o którym mowa w art. 11 ust. 1 pkt 4 UKSC;
8) nie wykonanie obowiązku, o którym mowa w art. 11 ust. 1 pkt 5 UKSC;
9) nie usuwanie podatności, o których mowa w art. 32 ust. 2 UKSC;
10) nie wykonanie obowiązku, o którym mowa w art. 14 ust. 1 UKSC;
11) nie przeprowadzenie audytu zgodnie z UKSC;
12) uniemożliwianie lub utrudnianie wykonywania kontroli, o której mowa w art. 53 ust. 2 pkt 1 UKSC;
13) nie wykonanie w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1 UKSC

- może nałożyć na operatora usługi kluczowej karę pieniężną określonych w art. 73 ust. 3 UKSC.

Jeżeli w wyniku kontroli kontroler Ministerstwa Klimatu i Środowiska stwierdzi, że operator usługi kluczowej uporczywie narusza przepisy ustawy, powodując:

1. bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
2. zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych,

- organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 1 000 000 zł.

Karę pieniężną, o której mowa w art. 73 UKSC, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.

UKSC reguluje również kwestię wysokości kar pieniężnych. Zgodnie z art. 73 ust. 3 wysokość kary pieniężnej, o której mowa w:

1) ust. 1 pkt 1, wynosi do 150 000 zł;
2) ust. 1 pkt 2, wynosi do 100 000 zł;

3) ust. 1 pkt 3, wynosi do 50 000 zł;
4) ust. 1 pkt 4, wynosi do 15 000 zł;
5) ust. 1 pkt 5, wynosi do 50 000 zł;
6) ust. 1 pkt 6, wynosi do 15 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu;
7) ust. 1 pkt 7, wynosi do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego;
8) ust. 1 pkt 8 i 9, wynosi do 20 000 zł;
9) ust. 1 pkt 10, wynosi 100 000 zł;
10) ust. 1 pkt 11 i 13, wynosi do 200 000 zł;
11) ust. 1 pkt 12, wynosi do 50 000 zł;
12) ust. 2 pkt 1, wynosi do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego;
13) ust. 2 pkt 2 i 3, wynosi do 20 000 zł.

UKSC określa również minimalną wysokość kary. Zgodnie z art. 74 ust. 4 kara, o której mowa w:

1) ust. 1 pkt 4, nie może być niższa niż 1000 zł;
2) ust. 1 pkt 1-3, 6-9 i 12, nie może być niższa niż 5000 zł;
3) ust. 1 pkt 5, 10, 11 i 13, nie może być niższa niż 15 000 zł.

Dodatkowo, zgodnie z UKSC, organ właściwy do spraw cyberbezpieczeństwa może nałożyć karę pieniężną na kierownika operatora usługi kluczowej w przypadku, gdy nie dochował należytej staranności celem spełnienia obowiązków, o których mowa w art. 8 pkt 1, art. 9 ust. 1 pkt 1 oraz art. 15 ust. 1 UKSC, z tym że kara ta może być wymierzona w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia.

Ustawodawca dał również możliwość organowi właściwemu ds. cyberbezpieczeństwa, w tym przypadku Ministerstwu Klimatu i Środowiska, nałożyć karę pieniężna na podstawie innych przyczyn. Zgodnie z UKSC, kara, o której mowa w art. 73 UKSC, może zostać nałożona również w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli MKiŚ uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

15. Zakaz powtórnych kontroli o tożsamym przedmiocie

Organ kontroli nie przeprowadza kontroli, w przypadku gdy ma ona dotyczyć przedmiotu kontroli objętego uprzednio zakończoną kontrolą przeprowadzoną przez ten sam organ.

Powyższej zasady nie stosuje się w przypadku, gdy:

1) kontrola ma dotyczyć okresu nieobjętego uprzednio zakończoną kontrolą;
2) ponowna kontrola ma na celu przeciwdziałanie zagrożeniu życia lub zdrowia;
3) ponowna kontrola jest niezbędna do przeprowadzenia postępowania w sprawie stwierdzenia nieważności, stwierdzenia wygaśnięcia, uchylenia lub zmiany decyzji ostatecznej lub wznowienia postępowania w sprawie zakończonej decyzją ostateczną;
4) ponowna kontrola jest niezbędna do przeprowadzenia postępowania w związku z uchyleniem lub stwierdzeniem nieważności decyzji przez sąd administracyjny;

5) ponowna kontrola jest niezbędna do przeprowadzenia postępowania w celu sprawdzenia wykonania zaleceń pokontrolnych organu lub wykonania decyzji lub postanowień nakazujących usunięcie naruszeń prawa, w związku z przeprowadzoną kontrolą, albo do sprawdzenia wykonania wezwania, o którym mowa w art. 21a ust. 1, zobowiązania, o którym mowa w art. 21a ust. 2, lub weryfikacji powiadomienia, o którym mowa w art. 21a ust. 5 lub 6 UPP;
6) ponowna kontrola jest niezbędna do przeprowadzenia postępowania związanego ze złożeniem korekty rozliczenia objętego uprzednio zakończoną kontrolą;
7) organ kontroli poweźmie uzasadnione podejrzenie, że uprzednio zakończona kontrola została przeprowadzona z naruszeniem prawa mającym wpływ na wynik kontroli lub dowody, na których podstawie ustalono istotne dla sprawy okoliczności faktyczne, okazały się fałszywe lub protokół kontroli został sporządzony w wyniku przestępstwa;
8) po sporządzeniu protokołu kontroli z poprzedniej kontroli wyszły na jaw istotne dla sprawy nowe okoliczności faktyczne lub nowe dowody nieznane organowi administracji lub państwowej jednostce organizacyjnej w chwili przeprowadzenia kontroli, w tym wskazujące na wystąpienie nadużycia prawa, o którym mowa w art. 5 ust. 5 ustawy z dnia 11 marca 2004 r. *o podatku od towarów i usług* (Dz.U. z 2020 r. poz. 106, 568, 1065, 1106 i 1747);
9) przedsiębiorca prowadzi działalność w zakresie objętym nadzorem, o którym mowa w art. 1 ust. 2 ustawy z dnia 21 lipca 2006 r. *o nadzorze nad rynkiem finansowym*.

16. Załączniki

1. Załącznik nr 1 – Przykładowe dokumenty wskazane w regulacjach
2. Załącznik nr 2 – Wystąpienie o wyrażenie zgody na przeprowadzenie kontroli w siedzibie MKiŚ
3. Załącznik nr 3 – Zawiadomienie o zamiarze wszczęcia kontroli
4. Załącznik nr 4 – Weryfikacja prawdziwości oświadczeń
5. Załącznik nr 5 – Oświadczenie o bezstronności i poufności
6. Załącznik nr 6 – Harmonogram kontroli
7. Załącznik nr 7 – Wystąpienie o wyrażenie zgody na przeprowadzenie kontroli w sposób zdalny
8. Załącznik nr 8 – Upoważnienie do przeprowadzenia kontroli
9. Załącznik nr 9 – Rejestr kontroli OUK
10. Załącznik nr 10 – Protokół kontroli